Weekly Report: Week 1

The main work I have done in the past week was paper reading. I read the papers you gave me and found some papers according to my personal interests, and am now gaining some big picture of what I am going to do in the next few months.

First, I think I should give up the idea to make GNNs go deep. Actually it is an interesting topic for me, and has been raised as one of the most important open problem in this area(mentioned in both the survey from Liu Zhiyuan, Tsinghua and Philip Yu, UIC). But it is too challenging for me to finish such a job for the following reasons:

- **Too few related works**. To my best knowledge, I only found two. The work H-GCN I mentioned the other day can go as deep as 9 layers on Cora and 11 on Reddit, they use a novel pooling method to avoid over-smoothing. And another work called *can GCNs go as deep as CNNs* borrowed some popular methods from CV, i.e., Resnet, Densenet, and Dilated Convolution, and reaches 56 layers. But its task is a typical CV task, point cloud semantic segmentation. Not so sure whether it will work for DM tasks, since in the appendix of Thomas Kipf's GCN paper residual learning has already been used and proved not so useful.
- **High demands for hardware resources**. To make deep GCNs we may need more GPU resources than we have, so it is not so possible.

Second, I found the adversarial attack & defense of GNNs a very promising field, but the problem setting is too open at this period of time. I read the papers and a survey from Philip Yu's team, realizing the problem formulations are far from united. People use quite different definitions, for example, the metric to evaluate perturbation, the knowledge attackers have, the tasks the attacked models do, the dataset they use... As a novice in this field, I think this problem will be too challenging for me.

The most interesting paper for me in the list is the Robust GCN by Cui Peng's team. I found this interesting for two reasons:

- Its goal is to improve the robustness of the GCN model, but does not **consider the attack method**. So the improvement is general. Also, it gives me an impression that doing such work does not necessarily require expertise in adversarial attack.
- The main idea is to **extend existing models instead of create a new one**. The existing models have been studied extensively, by just posing some modification on them can improve their robustness as well as enjoy their existing advantages.

My idea at this stage:

- I want to do some work in the field of robust GNNs. As a starter in scientific research, I think it will be better (and of course, easier) to do research based on previous intelligence. Robust models have been extensively investigated in CV and NLP, so I am considering borrowing some ideas from them and integrating with the GNN formulation.
- I want to build a general framework which can serve as a plug-and-play model. It should fit multiple existing GNN models and can improve their robustness without modifying their network structures. Such framework should be of great importance because it can be universally and easily applied. As far as I can think now, we may get embeddings from the original GNN models, and then do some fine-tune on the embeddings(it is just a rough idea for now).